REMARKS

The Examiner has rejected Claims 1-29 under 35 U.S.C. 102(b) as being anticipated by Nessett et al. (U.S. Patent No. 5,968,176). Applicant respectfully disagrees with such rejection, especially in view of the amendments made hereinabove. Specifically, applicant has amended each of the independent claims to further define scanning as "virus and content scanning of network traffic".

With respect to each of the independent claims, the Examiner has relied on the following excerpt from Nessett to make a prior art showing of applicant's claimed "wherein the processor is adapted for scanning network traffic transmitted between the computer and the network" (see this or substantially similar, but not identical, language in independent Claims 1, 14, 27, 28 and 29):

> "The use of filtering for security purposes can occur in NICs, Switches, Repeaters, Routers, and Remote Access Equipment. Filtering within a NIC can be used to ensure the source MAC addresses it sends are valid and that the source addresses it receives are from trusted end systems. However, NIC filtering can be used for other equally valid purposes, such as offloading VLAN enforcement processing from Hubs, implementing pervasive multilayer firewalls, and providing hardware support for higher level security protocols." (Col. 11, lines 54-62)

Applicant respectfully asserts that Nessett's disclosure of implementing a firewall on a network card is in no way even a suggestion of applicant's claimed processor that is adapted for scanning network traffic. A firewall, by definition, is a system designed to prevent unauthorized access to or from a network. Thus, a firewall does not explicitly or inherently scan network traffic. Also, according to Nessett:

> "When each NIC, such as the NIC at end system 601, receives these rules, it discards all of those node specific policy rules for which its end system (e.g., 601) is not a destination. It then uses the remaining rules to filter packets arriving at the end system (e.g., 601). In this example, the end systems 601, 602,and 603, with NICs enforcing node specific policy rules, would not be able to receive any traffic other than FTP requests from end

> systems 611 and 612 in Host Group Two 610." (Col. 23, lines 18-26)

In the above excerpt, Nessett explicitly discloses utilizing rules to filter packets arriving at an end system, where an example of such a rule may include only allowing FTP requests. This filtering process simply does not meet applicant's claimed scanning network traffic.

To further clarify this paramount distinction, applicant has amended each of the independent claims to further define scanning as "virus scanning and content scanning of network traffic...wherein the virus scanning utilizes virus signature files to scan for known types of malicious programs or data" (see this or substantially similar, but not identical, language in independent Claims 1, 14, 27, 28 and 29).

Again, applicant argues that neither virus scanning nor content scanning as claimed by applicant is taught by a firewall on a network card, and especially not where the virus scanning utilizes virus signature files to scan for known types of malicious programs or data. Specifically, for example, virus scanning, by definition, involves a utility that searches for viruses, and optionally removes any that are found. Such functionality is simply not met by Nessett's firewall that solely prevents unauthorized access. Since network adapters are often ingress points for many untrusted files and data that may proliferate on an associated computer, virus and content scanning network traffic on a processor positioned on a network adapter creates an enhanced layer of security at the network adapter.

Still yet, applicant brings to the Examiner's attention the subject matter of new Claims 30-34 below, which have been added for full consideration:

"wherein the content scanning enforces operational policies of an organization" (see Claim 30);

"wherein the policies include detecting entities selected from the group consisting of harassing content, pornographic content, junk e-mails, and misinformation" (see Claim 31);

"wherein the virus signature files are stored on a non-volatile solid state memory on the network adapter" (see Claim 32);

"wherein the memory is user protected by configuring a network adapter BIOS with a password that only a user can change" (see Claim 33);

"wherein the received packets that are of interest include executable files" (see Claim 34).

A notice of allowance or a specific prior art showing of each of such claim limitations, in the context of the remaining elements, is respectfully requested.

Thus, all of the independent claims are deemed allowable. Moreover, the remaining dependent claims are further deemed allowable, in view of their dependence on such independent claims.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 505-5100. The Commissioner is authorized to charge any additional fees or credit any overpayment to Deposit Account No. 50-1351 (Order No. NAI1P056/01.187.01).

Respectfully submitted,
Zilka-Kotab, PC.

Kevin J. Zilka
Registration No. 41,429

P.O. Box 721120
San Jose, CA 95172-1120
408-505-5100